

# Determining FPKI Compliance to IETF-PKIX

David Simonetti

FPKI Technical Working Group

November 12, 1998



# Outline

- Introduction to X.509 and the Profiles
- Definition of Compliance
- The Result of the Analysis
- Analysis Extension by Extension
- Summary and Next Steps



# X.509 Profiles

- X.509 Is ISO Standard for Public Key Certificates
- X.509 Provides A Number of Implementation Options
- Profiles Determine Specific Implementation Based On Community Requirements
- IETF-PKIX Is The Internet Community



# Compliance

- Compliance Based Upon
  - Inclusion of All Required Elements
  - Exclusion of All Prohibited Elements
  - Certificate and CRL Processing Based on PKIX and X.509



# The Result

- FPKI Is Currently *Not Compliant* With PKIX



# The Certificate Extensions



# Authority Key Identifier

- Required in Both Profiles
- Both Constrain Use to *keyIdentifier*
- PKIX Recommends Deriving *keyIdentifier* From Public Key
- FPKI Derives Using SHA-1 Hash of Public Key
- FPKI is PKIX Compliant



# Subject Key Identifier

- Required in Both Profiles in All CA Certificates
- Both Derive *keyIdentifier* From Public Key
- FPKI is PKIX Compliant



# Key Usage

- Required in Both Profiles as “Critical”
- *keyUsage* Definitions Are Similar But Not Identical
- FPKI Restricts *keyUsage* Combinations During Generation
- FPKI Adds Processing Requirements



# Key Usage (cont.)

- Suggest:
  - Adopt PKIX Definitions
  - Retain Combination Restrictions
  - Retain Processing Requirements, But Restate *digitalSignature* and *nonRepudiation* Based On PKIX Definitions
- Suggestions Result in PKIX Compliance With Additional FPKI Requirements



# Extended Key Usage

- FPKI Indicates No Requirements
- PKIX Defines Extended Key Usages, But Does Not Require Support
- Recommend Adopting PKIX Extended Key Usages, But Indicate That Support Is Optional



# Private Key Usage Period

- FPKI Indicates No Requirements
- PKIX Recommends Against Use
- FPKI is PKIX Compliant



# Certificate Policies

- FPKI Requires This Extension As “Critical”
- PKIX Does Not Indicate a Recommendation
- PKIX Defines Qualifiers; FPKI Adopts Them
- FPKI Is PKIX Compliant



# Policy Mappings

- FPKI Requires Support
- PKIX Allows Support (“may be supported”)
- FPKI Is PKIX Compliant; But FPKI Adds Requirement for Support



# Subject/Issuer Alternative Name

- PKIX Allows The Extension To Be Critical
- FPKI Adds Requirements
  - Extension Must Be Non-Critical
  - Constrained to *dNSName*, *directoryName*, and *uniformResourceIdentifier* (add *rfc822Name*?)
  - Reject A Cert With If This Extension Is Critical and Does Not Include a *directoryName*
- *Rejection of Otherwise Valid Cert Results In PKIX Non-Compliance*



# Subject Directory Attributes

- PKIX Does Not Recommend
- FPKI Support Is Optional
- May Carry MISSI-defined Access Control Attributes If Needed
- FPKI is PKIX Compliant



# Basic Constraints

- Must Appear As A Critical Extension In Both Profiles
- Only For CA Certs; Not Recommended in EE Certs
- FPKI Is PKIX Compliant



# Name Constraints

- Must Appear As A Critical Extension In All CA Certificates In Both Profiles
- PKIX Restricts Against Using *minimum* and *maximum*
- FPKI Adds Requirements:
  - Restricts Name Constraints to *directoryName*
  - Rejects A Cert If This Extension Is Critical And Contains Constraints Other Than *directoryName*
- *Rejection of Otherwise Valid Cert Results in PKIX Non-Compliance*



# Policy Constraints

- PKIX Does Not Make Any Support Recommendations
- FPKI Requires It Be Critical
- FPKI Is PKIX Compliant



# CRL Distribution Points

- PKIX Recommends Support As a Non-Critical Extension (Does Not Require)
- FPKI Requires It As A Critical Extension
- FPKI Restricts distributionPoints to *directoryName* and *uniformResourceIdentifier*
- FPKI Is PKIX Compliant



# Authority Information Access

- PKIX Private Extension
- May Be Included In Subject Or CA Certs
- Must Always Be Non-Critical
- FPKI Does Not Support
- FPKI Is PKIX Compliant



# Certification Path Validation

- FPKI Indicates Initial Values for Cert Path Processing Variables
- FPKI Lists Notifications For Expired Certificates And Provides the Option To Continue Processing
- FPKI Checks for Non-Empty Subject and Issuer Fields (Though PKIX Requires Non-Empty Subject and Issuer Fields In CA Certs)
- FPKI Ignores Unique Ids; PKIX Recommends Parsing and Comparing Unique Ids
- *FPKI Is Non-Compliant*



# The CRL and CRL Entry Extensions



# Authority Key Identifier

- Required By Both PKIX and FPKI
- Both Require Use of *keyIdentifier*
- FPKI Is PKIX Compliant



# Issuer Alternative Name

- FPKI Requires Support for Name Types *dNSName* and *uniformResourceIdentifier*
- PKIX Recommend Non-Critical; FPKI Requires Non-Critical
- Rejects A Cert If This Extension Is Critical And Contains Other Than *directoryName*
- *Rejection of Otherwise Valid Cert Results in PKIX Non-Compliance*



# CRL Number

- PKIX Requires In All CRLs
- Optional for FPKI
- *FPKI Is Non-Compliant*



# Delta CRL Indicator

- PKIX Makes No Recommendations
- FPKI Specifies No Support Requirements
- FPKI Is PKIX Compliant



# Issuing Distribution Point

- PKIX Makes No Recommendations
- FPKI Requires For ICRLs
- FPKI Is PKIX Compliant



# Reason Code

- Both PKIX and FPKI Strongly Recommend Use
- FPKI Is PKIX Compliant



# Hold Instruction Code

- PKIX Defines Several Instruction Codes
- PKIX Requires Processing of Two Codes
- FPKI Does Not Require Support
- *FPKI Is Non-Compliant*



# Invalidity Date

- PKIX Strongly Encourages Use
- FPKI Requires Use
- FPKI Is PKIX Compliant



# Certificate Issuer

- PKIX Recommends That Implementations Recognize This Extension
- FPKI Requires This Extension For ICRL Entries
- FPKI Is PKIX Compliant



# Algorithm Support

- PKIX Supports:
  - MD2, MD5, SHA-1 Hashes
  - RSA, DSA Signature Algorithms
  - RSA, Diffie-Hellman KM Algorithms
- FPKI Supports FIPS-Approved Algorithms
  - DSA and SHA-1



# Summary

- The Desire...“The FPKI Complies with PKIX and states the following additional requirements”
- FPKI Additional Requirements
  - Key Usage
    - Combination Restrictions
    - Processing Requirements
  - Support Certificate Policies Extension as “Critical”
  - Support of Policy Mappings Extension



# Summary (cont.)

- FPKI Additional Requirements (cont.)
  - Reject Critical Subject/Issuer Alternative Name Not Using *directoryName*
  - Reject Critical Name Constraints Not Using *directoryName*
  - Support Policy Constraints Extension As “Critical”
  - Support CRL Distribution Points Ext As “Critical”
  - Certification Path Processing Requirements
  - Support of Issuing Distribution Points CRL Extension
  - Support of Certificate Issuer CRL Entry Extension



# Next Steps

- Can We Overcome Non-Compliance Issues
  - Alternative Name and General Name Processing
  - Cert Path Validation Requirements
  - CRL Number and Hold Instruction Codes
- If So, Rewrite To Reflect PKIX Profile
- If Not, Update To At Least More Closely Align With PKIX

